Tik-79.159 Tiedon salaus ja suojaus	
Tentti 5 / spring '98	Tuomas Aura

Kirjoita vastauspaperiin opintojakson numero ja nimi, päivämäärä, nimesi, opintokirjan numero, osasto ja vuosikurssi.

Vastaa enintään **viiteen** (5) tehtävään. (Muuten tehtävä 6. jätetään arvostelematta.)

1. Määrittele tai selitä seuraavat käsitteet:
   (a) *Message Authentication Code* (MAC) (1p)
   (b) EDE-moodi (1p)
   (c) konfuusio (1p)
   (d) hybridisalaus (1p)
   (e) subliminaalinen kanava (1p)
   (f) *man-in-the-middle* -hyökkäys (1p)

2. Selitä, mistä seuraavat asiat johtuvat:
   (a) Salaus ei suojaa suojaa sanomien eheyttä. (Anna esimerkki lohkosalauksesta ja julkisen avaimen salauksesta.) (2p)
   (b) Salattavaan sanomaan pitää yleensä lisätä satunnaisuutta jossain muodossa. Kerro myös, miten satunaisuutta voidaan lisätä lohkosalauksessa ja RSA:ssa. (2p)
   (c) Kahden kierroksen Feistel-salaus ei ole turvallinen. (2p)

3. Diffie–Hellman-parametrien arvoiksi on sovittu $n = 2113$ ja $g = 5$. Vastaanotat A:lta sähköpostitse **asianmukaisesti allekirjoitetussa** sanomassa hänen julkisen DH-avaimensa $X = 991$. Arvot omaksi salaiseksi avaimeksesi $y = 131$.
   (a) Millä sanomilla avaintenvaihtoprotokolla jatkuu? (2p)
   (b) Mikä tulee yhteiseksi salaiseksi avainmateriaaliksi? (2p)
   (c) Miksi sanomat pitää allekirjoittaa? (2p)

4. Julkisen avaimen Needham-Schröder (oletetaan, että osapuolet jo tuntevat toistensa julkiset avaimet):

1.	$A \longrightarrow B$	$E_B(N_A, A)$
2.	$B \longrightarrow A$	$E_A(N_A, N_B)$
3.	$A \longrightarrow B$	$E_B(N_B)$

   Nonsseista generoidaan istuntoavain $K_{ses} = h(N_A, N_B)$.
   (a) Mistä A saa nonssin N_A? (1p)
   (b) Anna esimerkki algoritmeista, joilla funktio E voitaisiin toteuttaa. (1p)
   (c) Mikä vakava hyökkäys protokollaa vastaan on mahdollinen? (Vihje: kun A ottaa yhteyden B:hen, B voi esiintyä C:lle A:na. Esitä hyökkäyksen kulku yksityiskohtaisesti.) (2p)
   (d) Miten protokollan voi korjata? (1p)
   (e) Onko autentikointi korjatussa protokollassa implisiittinen vai eksplisiittinen? (perustele) (1p)

5. Steganografia ja sen merkitys käytännössä. (6p)

6. Nollatietotodistukset. (6p)

Tik-79.159 Cryptography and data security
Examination 5 / spring '98 — Tuomas Aura

Write on the answer sheet the number and name of the course, today's date, your name, student number, department and class number.

Answer at most **five** (5) questions. (Otherwise, question 6 will not be graded.)

1. Define or explain the following terms:
   (a) Message Authentication Code MAC (1p)
   (b) EDE mode (1p)
   (c) confusion (1p)
   (d) hybrid encryption (1p)
   (e) subliminal channel (1p).
   (f) *man-in-the-middle* attack (1p)

2. Explain, why the following claims are true:
   (a) Encryption does not protect the integrity of messages. (Give an example for block ciphers and for public key encryption.) (2p)
   (b) Usually randomness should be added to messages before encryption. Describe also how randomness can be added in a block cipher and in RSA. (2p)
   (c) Two-round Feistel encryption is not secure. (2p)

3. You have agreed with secret agent A to use Diffie–Hellman key exchange with parameters $n = 2113$ and $g = 5$. You receive in a **properly signed** message from A her public DH key $X = 991$. You randomly choose your own private key to be $y = 131$.
   (a) With which messages does the key exchange protocol continue? (2p)
   (b) What will be the shared secret key? (2p)
   (c) Why must the messages be signed? (2p)

4. Public-key Needham-Schröder (we assume that the parties know each other's public keys):

1.	$A \longrightarrow B$	$E_B(N_A, A)$
2.	$B \longrightarrow A$	$E_A(N_A, N_B)$
3.	$A \longrightarrow B$	$E_B(N_B)$

   A session key is generated from the nonces: $K_{ses} = h(N_A, N_B)$.
   (a) Where does A get the nonce N_A from? (1p)
   (b) Give an example of algorithms with which the function E could be implemented. (1p)
   (c) What serious attack is possible against the protocol? (Hint: when A contacts B, B can pose as A to C. Present details of the attack.) (2p)
   (d) How can the protocol be repaired (1p)
   (e) Is the authentication in the repaired protocol implicit or explicit? (explain why) (1p)

5. Steganography and its practical implications. (6p)

6. Zero-knowledge proofs. (6p)